Anti-financial crime policy

Status of document:	Live	
Version:	2.1	
Approved by:	Council	
Date of approval:	28/02/18	
Effective from:	28/02/18	
Owner:	Nicola Ebdon, Head of Governance	
Author:	Howard Miller, Governance Manager	
Relevant legislation:	Anti-Terrorist Crime and Security Act 2001 Bribery Act 2010 Counter-Terrorism Act 2008 Criminal Finances Act 2017 Fraud Act 2006 Money Laundering Regulations 2007 Proceeds of Crime Act 2002 Terrorism Act 2000	
Linked policies:	Code of Conduct Contracts and Procurement Policy Gifts and Hospitality Policy Investigation Policy Management of Interests Policy Member appointment and reappointment Policy Recruitment Policy Speaking Up (Whistleblowing) Policy Standards of Conduct, Attendance and Performance	
Next policy review date:	**02/2021**	
Location - Website:	*(hyperlinks of where the policy is published)*	
Updates made:	**February 2018**	Replaces 'Anti-bribery, money laundering, fraud, theft and corruption' policy

Contents

1. Statement

1.1. We have a zero tolerance policy towards bribery, money laundering, fraud, theft and terrorist financing (collectively referred to in this policy as ‘financial crime’). We are committed to preventing, detecting and eliminating financial crime and fostering a culture in which any such activity is considered unacceptable. We will consistently apply the letter and spirit of all relevant legislation in all of our work.

1.2. We expect all those we engage with including our members, advisors, visitors, consultants and employees (known collectively in this policy as “members and employees”), and our stakeholders, contractors, suppliers and registrants to comply with this approach when carrying out their duties for and on behalf of the GOC or working with us.

1.3. We will investigate all reported cases and take the appropriate action, including reporting to the appropriate authorities, disciplinary action, prosecution and active pursuit of recovery.

1.4. We also expect others working with us or on our behalf, for example consultants and third parties, to have in place their own policy and procedures to prevent and detect financial crime.

1.5. Our policy has been endorsed by the GOC Chief Executive and Registrar and Council and has been communicated to everyone in our organisation to ensure their commitment and compliance. Our senior management attaches the utmost importance to this policy and as stated above will apply a "zero tolerance" approach to acts of financial crime by anyone who works for us, with us or on our behalf.

2. Purpose

2.1. This policy:

2.1.1 defines financial crime and provides examples (see annex one) which can use be used to recognise such activity; and

2.1.2 sets out our expectations in relation to the prevention, detection and reporting of financial crime and the consequences of non-compliance with this policy.

3. Scope

3.1. This policy applies to all members, employees, advisors and visitors.

3.2. We also expect others working with us, or on our behalf, for example, consultants, suppliers, stakeholders and registrants, to comply with this policy

and ensure that they are aware of their own organisation's policy and procedures to prevent and detect financial crime.

4. Glossary of terms

4.1. **Bribery** means offering, promising or giving someone a financial or other advantage to encourage them to perform their functions or activities improperly, and includes where it is known or believed that the acceptance of the advantage in itself constitutes improper performance. It also means asking for or agreeing to accept a bribe. It includes facilitation payments (small bribes paid to speed up a service).

4.2. Money laundering means the process of turning the proceeds of crime into property or money that can be accessed legitimately without arousing suspicion.

4.3. Fraud is a form of dishonesty, involving either false representation, failing to disclose information or abuse of position, undertaken in order to make a gain or cause loss to another. Among the most common types of fraud are:

- income-related fraud;
- expenditure fraud;
- property and investment fraud;
- procurement fraud;
- fraudulent fundraising in the organisation's name;
- fraudulent invoicing and grant applications;
- identity fraud/theft;
- banking fraud; and
- e-crime.

4.4. **Theft** is dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it and includes associated offences such as false accounting.

4.5. **Terrorist financing** is the raising, moving, storing and use of financial resources for the purposes of terrorism

5. Prevention and detection

5.1. We expect all those we engage with to:

5.1.2 comply with this policy and other policies which have a bearing on this area of work, for example (this list is not exhaustive) policies on recruitment, appointments, contracts and procurement, management of interests and the receipt and provision of gifts and hospitality;

5.1.3 have, and be seen to have, the highest standards of honesty, propriety and integrity in the exercise of their duties;

5.1.4 report all suspected and known cases of financial crime; and
5.1.5 assist in any investigation.

5.2. We will:
5.2.1 publish a statement setting out our commitment to preventing financial crime;
5.2.2 undertake a risk assessment of our exposure to potential external and internal risks;
5.2.3 ensure we have suitable levels of internal controls embedded in our day to day practices, particularly in relation to financial procedures;
5.2.4 ensure our other policies (which include, but are not limited to recruitment, appointments, contracts and procurement and gifts and hospitality) are clear on our commitment to preventing and detecting financial crime and are followed;
5.2.5 ensure that references are checked and necessary due diligence is carried out when recruiting and appointing members and employees and when we bring in new suppliers;
5.2.6 ensure our members and employees and others we engage with are aware of their duties in relation to the management of interests and the receipt and provision of gifts and hospitality and understand how this policy and all related policies apply to them;
5.2.7 ensure there are appropriate processes in place to report concerns regarding financial crime;
5.2.8 ensure there are appropriate processes in place to effect prompt investigation upon receipt of concerns;
5.2.9 ensure an appropriate whistleblowing policy is in place;
5.2.10 provide training and guidance as necessary in order for people to understand their role in relation to preventing, detecting and reporting financial crime;
5.2.11 record and report on allegations received under this policy; and
5.2.12 take appropriate disciplinary and legal action if and when necessary such as dismissal, removal from office and termination of contract.

6. Compliance

6.1. Compliance with this policy is mandatory.

6.2. Non-compliance by:
6.2.1 employees may be considered to be gross misconduct and could result in summary dismissal in accordance with the Conduct, Attendance and Performance policy;
6.2.2 members is a breach of the Code of Conduct which could result in their removal from office;

6.2.3 consultants and suppliers could result in termination of their contract with us;
6.2.4 registrants could result in them being reported to their employer; and
6.2.5 others we engage with such as stakeholders could be reported to any appropriate organisation or regulator.

6.3. If you have been offered a bribe or have any suspicions regarding financial crime or any concerns about conduct which you feel may have breached this policy you should:
6.3.1 if an employee (other than the Chief Executive and Registrar or a Director), report your concerns to your Director (or, if not appropriate, the Chief Executive and Registrar);
6.3.2 if a Director, report your concerns to the Chief Executive and Registrar (or, if not appropriate, the Chair of Council);
6.3.3 if the Chief Executive and Registrar, report your concerns to the Chair of Council (or, if not appropriate, the Senior Council Member);
6.3.4 if a member, report your concerns to your Chair (or, if not appropriate, the Chair of Council or, if also not appropriate, the Senior Council Member);
6.3.5 if none of the above, report your concerns to the Head of Governance (or, if not appropriate, the Chief Executive and Registrar);
6.3.6 if none of the above seems appropriate, raise your concern using either the Speaking Up in the GOC (Whistleblowing) policy or the Raising Concerns with the GOC (Whistleblowing) policy, as appropriate;
6.3.7 document your concerns immediately, including all relevant details such as dates, times, places, details of phone conversations, names of those involved etc; and
6.3.8 not attempt to carry out an investigation yourself as this might damage any subsequent enquiry and could lead to a loss of evidence.

6.4. You will be expected to co-operate fully with the person(s) leading the investigation.

6.5. All allegations of non-compliance with this policy will be investigated thoroughly in accordance with the Investigation Policy[1].

6.6. In all instances we will:
6.6.1 listen to all concerns raised and treat every allegation seriously and confidentially;
6.6.2 (unless inappropriate to do so), notify the Chief Executive and Registrar, the Audit and Risk Assurance Committee (ARC) and the Chair of Council

[1] H:\01 Shared Resources\01.06 Policies & Procedures\1. CENTRAL HUB - Policies and Procedures\1. Corporate\Internal investigations policy.pdf

of all allegations and keep them appraised of the progress and outcome of any investigation;

6.6.3 produce a report which details any weaknesses in internal controls which contributed to the financial crime concerned and where necessary make recommendations to ARC for remedial action;

6.6.4 not ridicule, victimise or discriminate against those who raise a legitimate concern, irrelevant of whether it proves to be founded or not;

6.6.5 take action against those who deliberately make a false statement or accuse someone of financial crime for malicious purposes; and

6.6.6 notify the person who initially raised the concern of the outcome of the investigation and any remedial action to be taken.

7. Further concerns

7.1. If you are unhappy with the outcome of the investigation you can raise your concerns using either the Speaking Up in the GOC (Whistleblowing) policy or the Raising Concerns with the GOC (Whistleblowing), as appropriate, which also give details of how you can make a ‘wider disclosure’ to external agencies.

8. Annex

Annex one – Potential indicators of financial crime

Annex one: potential indicators of financial crime

The following examples are not exhaustive and are intended to be used as a guide to assist in recognising financial crime (Source: Serious Fraud Office):

- Abnormal cash payments being received or paid.
- Pressure exerted for payments to be made urgently or ahead of schedule.
- Payments being made through third party country (eg. goods or services supplied to country ‘A’ but payment is being made, usually to a company in country ‘B’).
- Abnormally high commission percentage being paid to a particular agency. This may be split into two accounts for the same agent, often in different jurisdictions.
- Private meetings with contractors or companies hoping to tender for contracts.
- Unusual gifts or cash being received.
- Individual rarely or never takes time off even if ill, or holidays, or insists on dealing with specific contractors him/herself.
- Abusing decision processes or delegated powers for certain individuals or organisations.
- Making unexpected or illogical decisions accepting projects or contracts, including agreeing contracts not favourable to the organisation either with terms or time period, without proper explanation.
- Unusually smooth process of cases or projects where individual does not have the expected level of knowledge or expertise.
- Unexplained preference for certain contractors during tendering periods.
- Bypassing normal tendering/contractors procedure including avoidance of independent checks on tendering or contracting processes.
- Invoices being agreed in excess of contract without reasonable cause.
- Authorising invoices without the required level of authority.
- Incomplete documents or records regarding meetings or decisions.
- Organisational procedures or guidelines not being followed.
- The payment of, or making funds available for, expenses on behalf of others.